DD WRT Virtual Access Point (Guest WiFi)

These are my personal notes so not very well redacted, feel free to make a better version.

Index

Introduction

A Virtual Access Point (VAP) is an extra virtual interface created on the same radio with a different Wireless Network Name (SSID) also referred to as a Guest WiFi.
The VAP is created on the same radio as the master interface, so it shares a lot of its properties e.g. same channel, but it can have a different password.
This is often used as a wireless guest network, for security reasons, routing reasons, or QoS reasons.

Depending on your needs you can separate the VAP from your main Network e.g. for Guest Network, this is called an unbridged setup, you then have different subnets which can be isolated from each other.

If you want clients of the VAP to see your main network then choose the simple bridged setup, this can be useful if you set your kids on this separate VAP and then turn it off at certain times (Radio scheduling).

A lot of instructions/wiki's are old and sometimes outdated, if you followed those it is recommended to start fresh so to reset to defaults first.

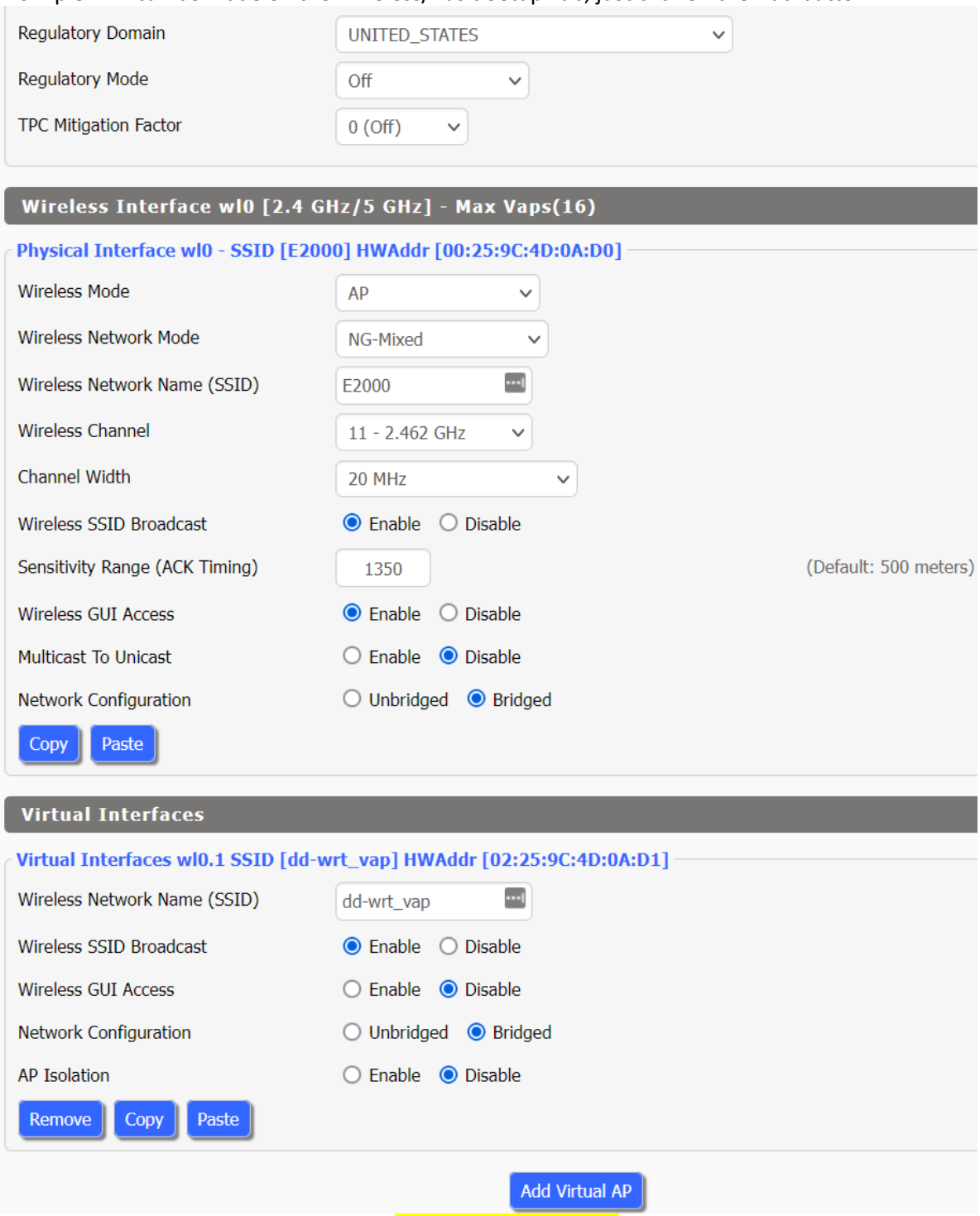
If you create your VAP on a on a **W**ireless **A**ccess **P**oint (WAP): a secondary router connected wired LAN<>LAN on the same subnet as the primary router, then first setup as a proper WAP and follow the instructions further down.
For a WAP there are also a lot of old and outdated instructions so if you have already used other instructions then best to reset to defaults and start fresh.

The Simple Setup is for adding just a single VAP, if you want to have more interfaces and or VLAN's tied together then use the Bridge Setup.

Simple Setup

Simple Bridged Setup (all clients can see each other)

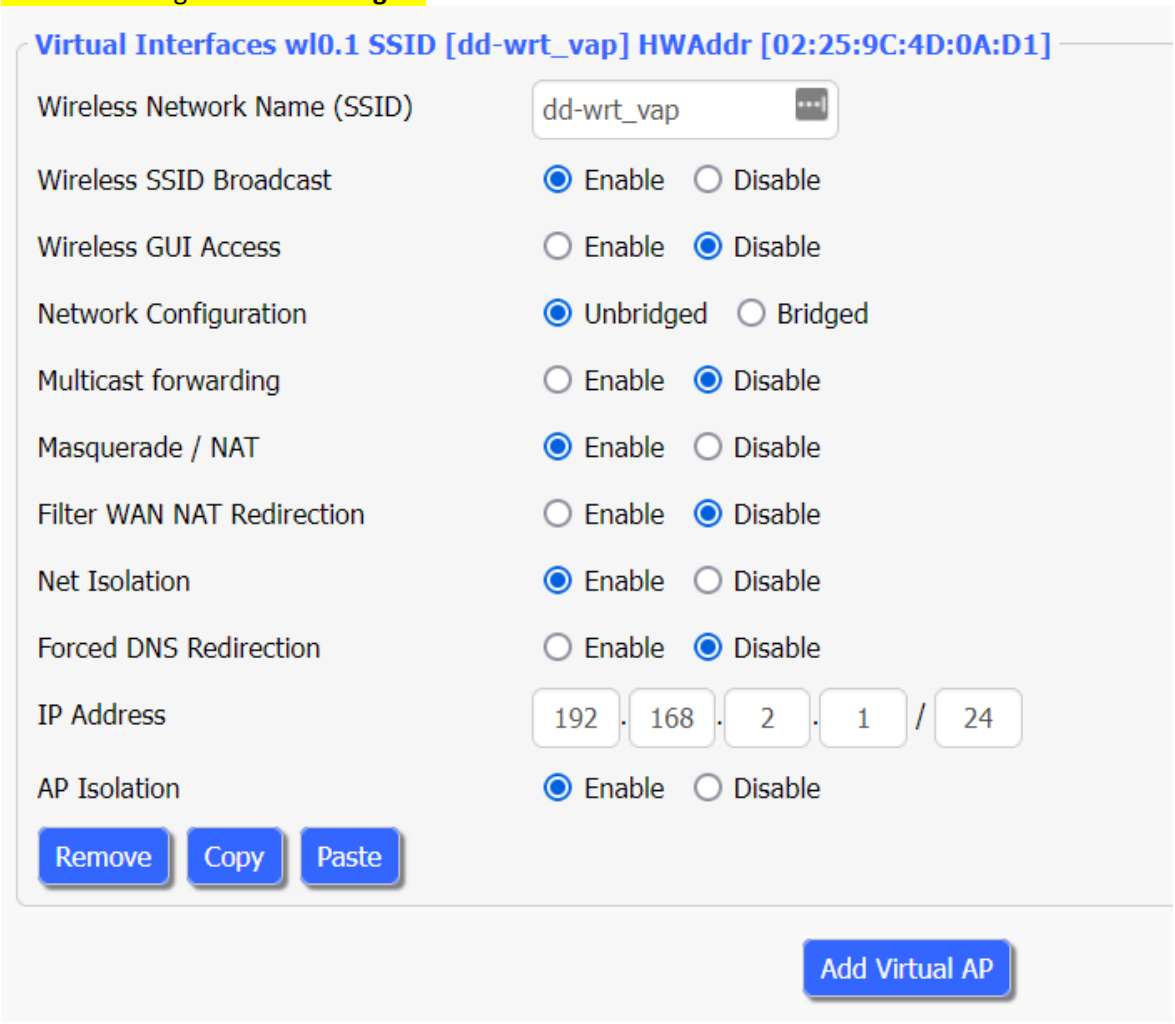
A simple VAP can be made on the Wireless/Basic Setup Tab, just click on the Add button.



After creating the VAP head over to the Wireless Security page and set the wireless security for the VAP.
For most routers wireless security must be set the same as for the primary interface (recommended is WPA2 Personal / CCMP-128 (AES).
If you want communication between your VAP and you existing network keep it Bridged under Network Configuration.

Separate Unbridged Setup

If you want the VAP separated from your main network (and if used for guest you do not trust, you should) then tick: Network Configuration: **Unbridged.**



The unbridged VAP must use a different IP subnet, e.g. the IP address must be **different** i.c. outside the range of your main network (which is the default 192.168.1.1/24).
As we normally use a netmask of /24, that means the third number of the IP address should be different from the routers Local IP e.g. 192.168.2.1 while the routers Local IP is 192.168.1.1

If you do not want that the wifi clients on the guest VAP can see each other than tick **AP Isolation: Enable**.

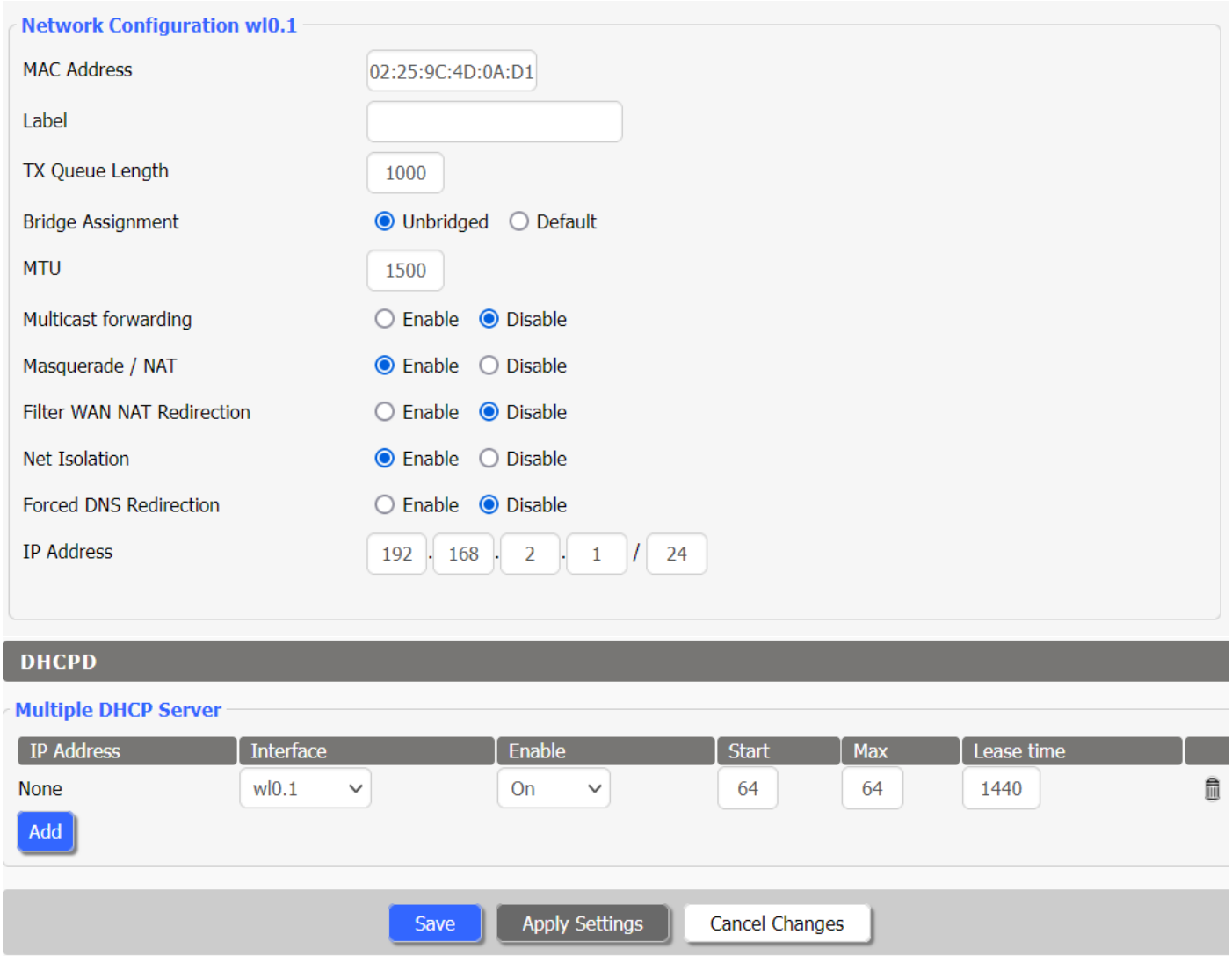
In this example the **Wireless GUI Access** is **Disabled** but enabling Net Isolation already disables GUI access.

If you do not want the clients on the guest VAP to see your home Network tick **Net Isolation: Enable** (recommended setting, you need at least build 49934, earlier builds had a bug which prevents proper isolation)**.**
Note: Net isolation only isolates between main subnet (br0) and VAP.
If you have more than one VAP the VAP's are not automatically isolated from each other and you have to do that manually

If you want a different DNS server for your VAP clients you can specify one after you have **enabled** "Forced DNS redirection"
Save and Apply and wait at least two minutes before proceeding to give the router time to restart the necessary services.

After creating the VAP head over to the Wireless Security page and set the wireless security for the VAP.
For most routers wireless security must be set the same as for the primary interface (recommended is WPA2 Personal / CCMP-128 (AES)).

Now head over to the Setup/Networking tab , scroll to the bottom and click on Add, to add a DHCP server, which you bind to wl0.1 (**for Atheros routers it is wlan0.1**).
For easier use with CIDR notation set the start address at 64 for a max number of users of 64.



Note: when a VAP is setup on a Wireless Access Point, you will not see settings related to WAN.

After you are done: **REBOOT!**
Very important, when you are done you have to reboot otherwise you will not get a DHCP address

Note: Setup> Basic Setup > Optional Settings > Shortcut Forwarding Engine (SFE) is not compatible with VAP. It should be automatically disabled but this does not always happen on Broadcom routers, so disable it manually.

References:

@jwh's guide: https://www.dd-wrt.com/wiki/index.php/Guest_Network
https://sploitworks.com/bbs/showthread.php?tid=3
https://flashrouters.zendesk.com/hc/en-us/articles/115000967873-How-To-Setup-a-DD-WRT-Guest-Wireless-Network-On-Your-FlashRouter

Isolating VAP's:

Net Isolation

If you Enable "Net Isolation" the VAP/Bridge is isolated from the Main network.

AP Isolation

If you want to isolate the wifi clients on the VAP from each other you can Enable "AP Isolation"
This setting is only available directly on the wlan interface and works bridged and unbridged.

Manual Settings

https://pastebin.com/r4u62P0B , (you do not need the nat rule)
https://wiki.dd-wrt.com/wiki/index.php/Multiple_WLANs
When "Net Isolation" is enabled the VAP/Bridge is isolated from the Main network but if you have multiple VAPs/Bridges those are not isolated from each other, you have to do that manually:
VAPx is e.g. wl0.1, wlan1.1. br1 etc:
iptables -I FORWARD -i <VAP1> -o <VAP2> -m state --state NEW -j REJECT
iptables -I FORWARD -i <VAP2> -o <VAP1> -m state --state NEW -j REJECT

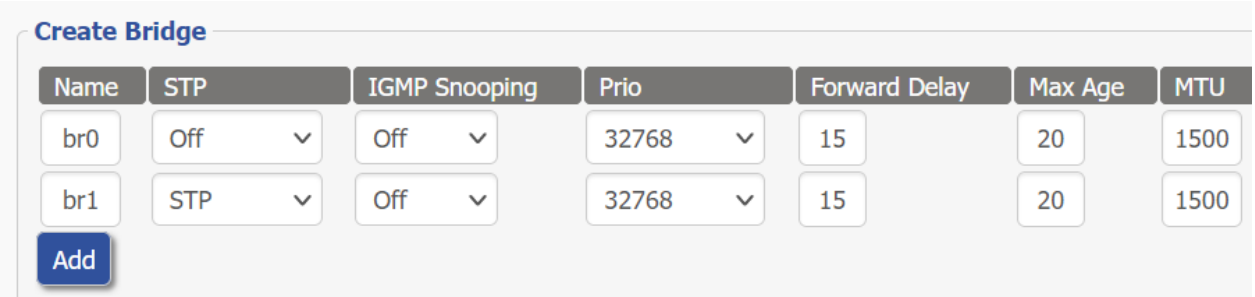
If you do want your VAPs to have local access but no Internet access than Disable Net isolation.
You can either Disable NAT on the interface (Setup/Networking) or use an iptables rule:
iptables -I FORWARD -i <VAPx> -o $(get_wanface) -j REJECT

Very useful are the instructions from @eibgrad: https://pastebin.com/r4u62P0B
Also with examples to give access to some clients e.g. printers on your main network

Bridge Setup

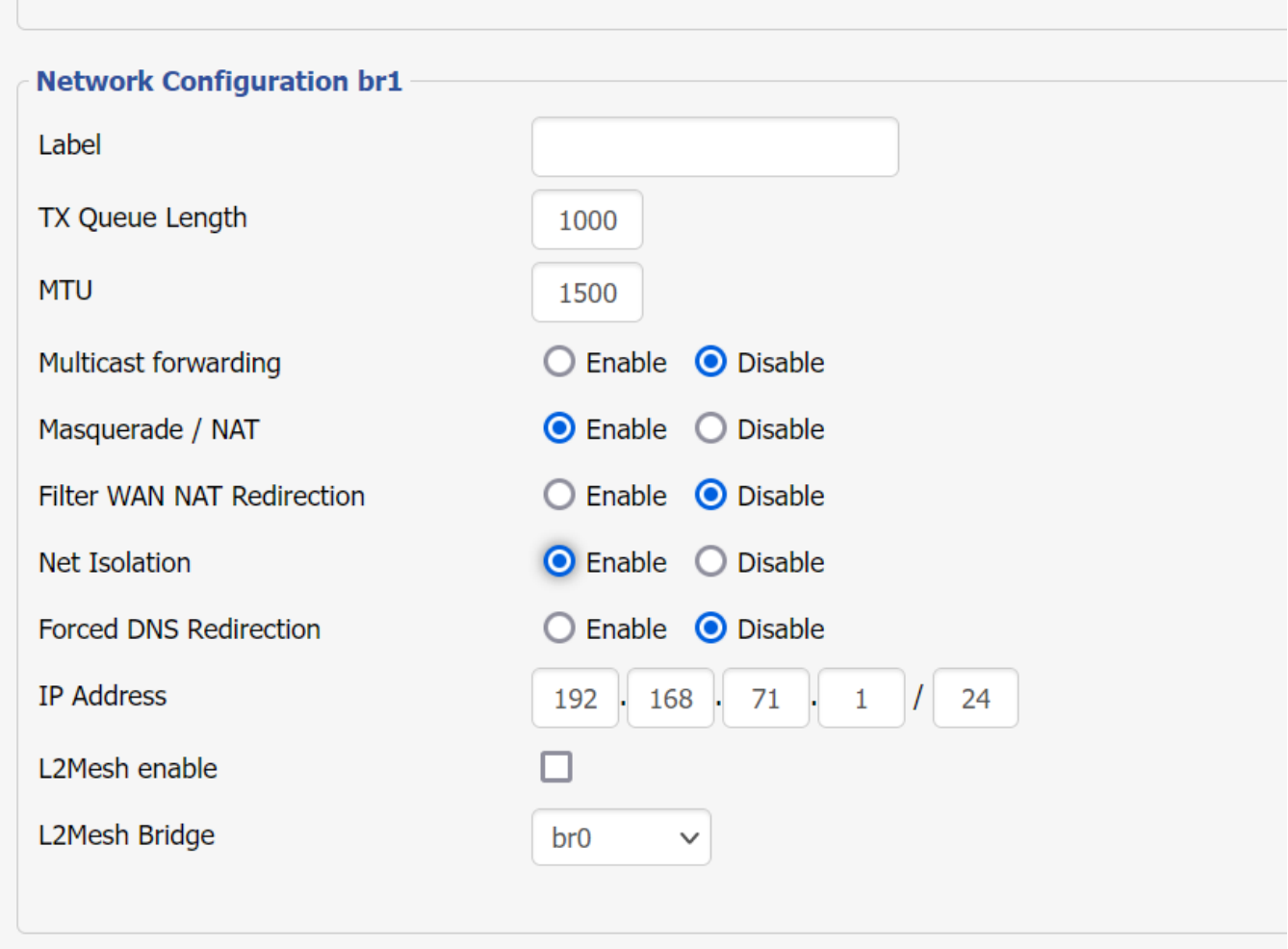
When you want to have more than one interface as Guest e.g. a second Wireless interface or ethernet ports (VLAN), you can tie this altogether on a newly made bridge.

Start with making the new bridge
On Network tab
Under Create Bridge click Add and name the bridge *br1*



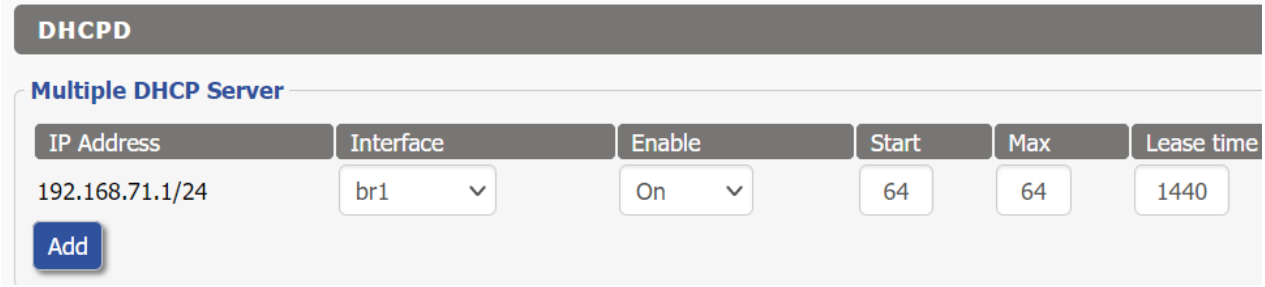
Save and Apply

After waiting at least two minutes to give the router time to restart necessary services, scroll down this page to the newly made bridge and give it an IP address different from the Local IP address, as we are using /24 subnet the third number (here 71) has to be different!
Enable Net isolation if this is for Guest/IoT access and you do not want guests on your regular network

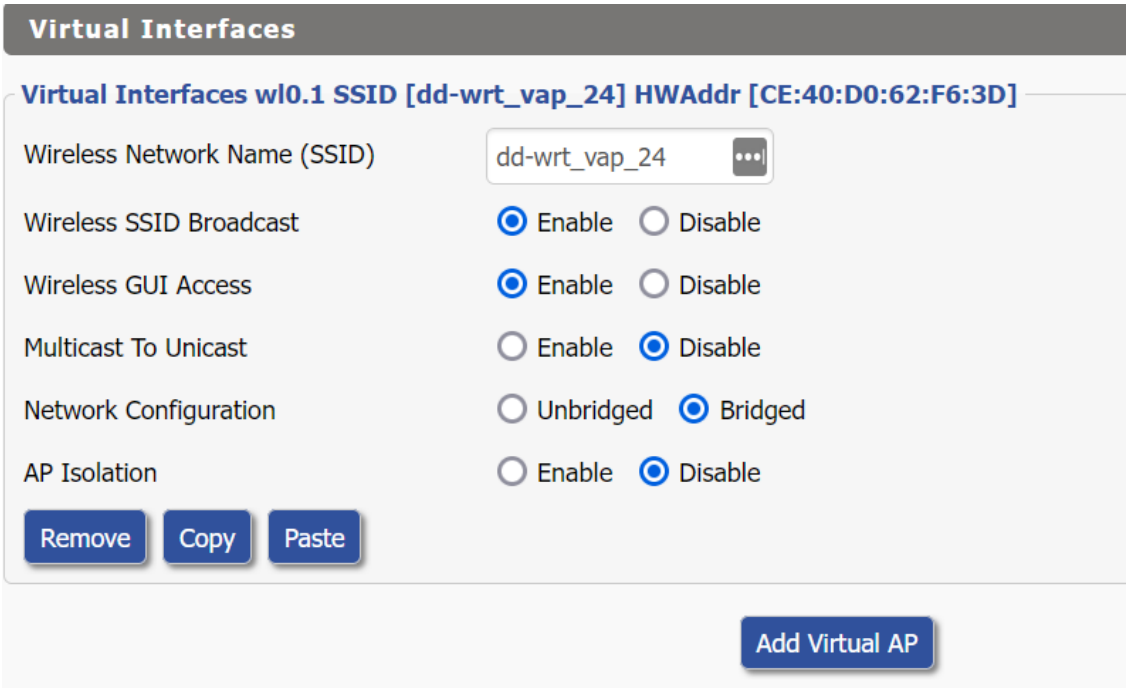


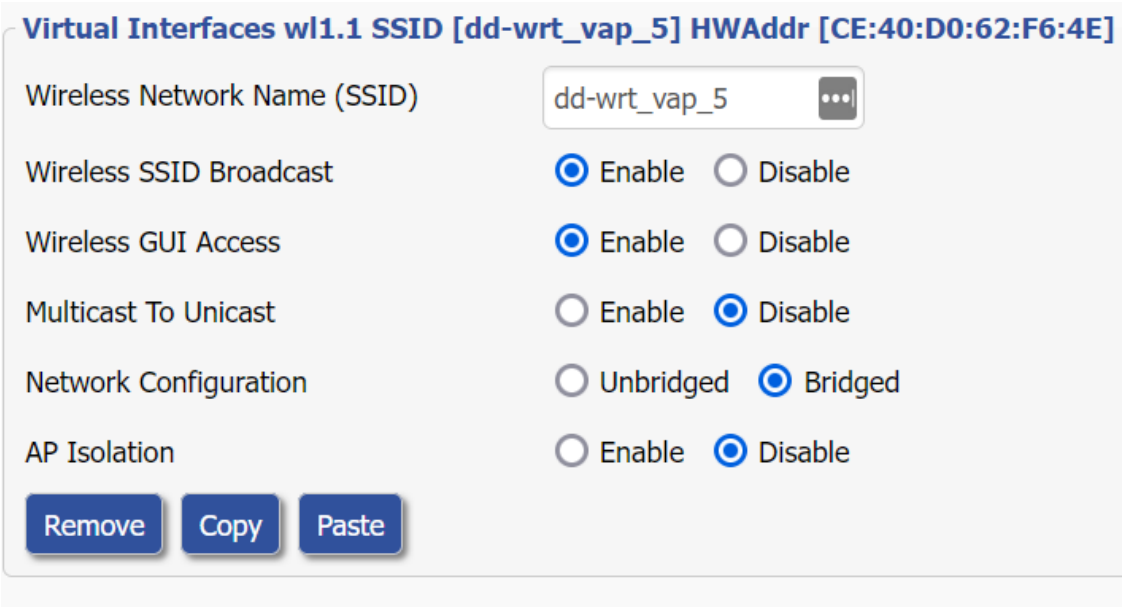
Save and Apply

Scroll down to the bottom of this Networking page and add a DHCPD server for br1, I use start at 64 for 64 leases (useful when doing things like Policy Based Routing).



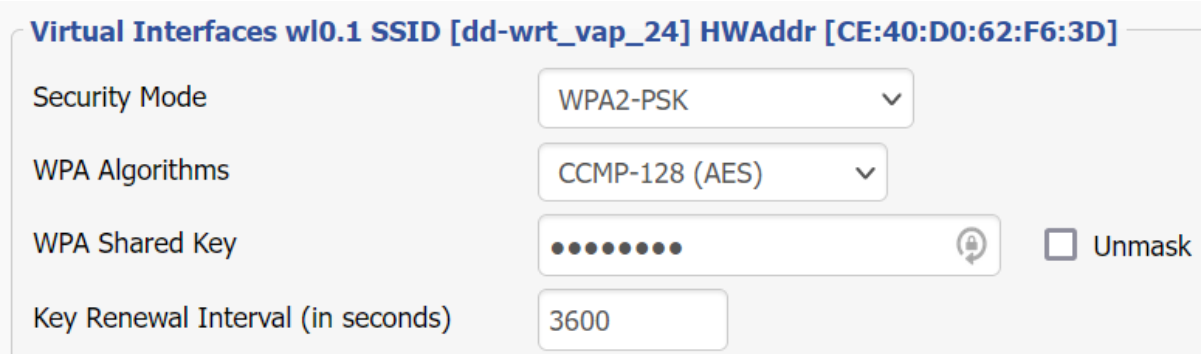
Now head back to the **Wireless Basic Setup page** and add one or more VAP's.
Leave the VAP's at default so leave them bridged!





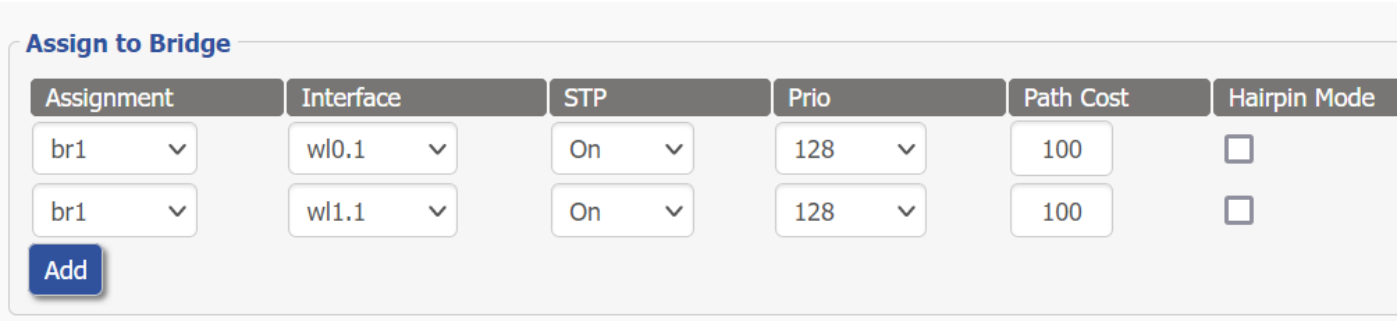
Save and Apply

Head over to the **Wireless Security page** and setup wireless security as WPA2 PSK (Personal) with CCMP-128 (AES) for all interfaces.



Now head back to the **Networking page**

Under Assign to Bridge Add both wl0.1 and wl1.1 (for Atheros they are wlan0.1 and wlan1.1) to br1



Save and Apply

After you are done a reboot is recommended

DNS

By default your clients will receive the DNS address of the VAP/bridge as their DNS server, DNSMasq will take it from there. So there is no need to set any DNS servers or make DNS related settings!

If you want to use another DNS server for your unbridged VAP/Bridge then you can use *Forced DNS Redirection*.
This uses iptables rules to DNAT traffic on port 53 to the desired DNS-server.
Alternatively you can set in Additional DNSMasq options:
dhcp-option=br1,option:dns-server,1.1.1.1,1.0.0.1

VAP on a WAP

If you place the unbridged VAP on a Wireless Access Point (WAP):
A secondary router connected wired LAN<>LAN on the same subnet as the primary router.
Setup:

- On Basic Setup page:
  - WAN disabled
  - DHCP server Disabled (=off and NOT set as Forwarder!)
  - Local IP address in subnet of primary router but outside DHCP scope, make sure the used IP address is unique on your network you cannot have duplicates.
    You can run udhcpc to give the WAP a static lease but because you can it doesn't mean you should ;)
  - Gateway **and** Local DNS pointing to primary router
    Example:
    If your primary router is 192.168.1.1 then set the Local IP address of the WAP to 192.168.1.**2** (make sure that is not used).
    The Gateway and Local DNS are set to point to the primary router e.g.: 192.168.1.**1**
- Keep DNSMasq enabled (both on Basic Setup page and Services page)
- On Setup > Advanced Routing, keep Operating mode in the default Gateway (the wiki says Router mode but do not do that, either it does not matter (this case) or break things)
- On Security > Firewall keep the **SPI Firewall enabled,** although you do not want a firewall it will be automatically disabled as there is no WAN so no need to change this setting from default.
- Connect LAN <> LAN (Although the WAN port is automatically added to the LAN bridge (br0) **better not use the WAN port** unless you really need that extra port, for most routers traffic still must use the CPU so performance is lacklustre and there are some routers where the WAN port is not added to br0 so the WAN port could be non-functional on some routers).

Note: For Broadcom routers for best throughput enable CTF on Basic Setup Page

If you have unbridged interfaces on the WAP (Virtual Access Point (VAP), bridge, vpn server or vpn cliente etc.), you have to add the following rule to the firewall in order to get internet access.
In the web-interface of the router (the WAP): Administration > Commands save Firewall:
#Always necessary (alternatively set static route on main router and NAT traffic from VAP/Bridge out via WAN):
iptables -t nat -I POSTROUTING -o br0 -j SNAT --to $(nvram get lan_ipaddr)

If you want to only have the VAP/bridge to have internet access and not access to the rest of the network
#Replace with the appropriate interface of your VAP, e.g. wl0.1, wlan0.1 etc:
GUEST_IF="wlan1.1"
#Net Isolation does not work on a WAP so keep it disabled, add for isolating VAP from main network:
iptables -I FORWARD -i $GUEST_IF -d $(nvram get lan_ipaddr)/$(nvram get lan_netmask) -m state --state NEW -j REJECT

#For isolating the WAP itself from the VAP/bridge:
iptables -I INPUT -i $GUEST_IF -m state --state NEW -j REJECT
iptables -I INPUT -i $GUEST_IF -p udp --dport 67 -j ACCEPT
iptables -I INPUT -i $GUEST_IF -p udp --dport 53 -j ACCEPT
iptables -I INPUT -i $GUEST_IF -p tcp --dport 53 -j ACCEPT

To make it simple and isolate the VAP/bridge from all know private subnets which isolate it not only from the main network but also from other bridges:

```
iptables -I FORWARD -i $GUEST_IF -d 192.168.0.0/16 -m state --state NEW -j REJECT
iptables -I FORWARD -i $GUEST_IF -d 10.0.0.0/8 -m state --state NEW -j REJECT
iptables -I FORWARD -i $GUEST_IF -d 172.16.0.0/12   -m state --state NEW -j REJECT
```

If you have a lot of VAP's bridges you can make a loop e.g.:

```
for GUEST_IF in br1 br2 br3
do
        iptables -I FORWARD -i $GUEST_IF -d $(nvram get lan_ipaddr)/$(nvram get lan_netmask)  -m state --state NEW -j REJECT
done
```

#Isolate the VAP/bridges from each other

```
iptables -I FORWARD -i br1 -o br2 -m state --state NEW -j REJECT
iptables -I FORWARD -i br2 -o br1 -m state --state NEW -j REJECT
```

Sometimes you see duplicate rules depending on how often the firewall restarts if that is a problem precede the rules with *-D* instead of *-I*.

note:
When the Wan is disabled VLAN 1 and VLAN2 are just bridged but on the switch level (swconfig) the VLANs are still separated

References:
@mrjcd's guide: https://forum.dd-wrt.com/phpBB2/viewtopic.php?p=1047143#1047143
https://wiki.dd-wrt.com/wiki/index.php/Guest_Network#VAP_with_no_WAN
ALternative DNSMAsq method: https://wiki.dd-wrt.com/wiki/index.php/Guest_Network#New_DNSMasq_Method
@eibgrad's isolation: https://pastebin.com/r4u62P0B